Exhibit B-7

Cybersecurity Law of the People's Republic of China [Effective]
中华人民共和国网络安全法 [现行有效]

【Print】

Issuing authority:	Standing Committee of the National People's Congress	**Document Number:**	Order No. 53 of the President
Date issued:	11-07-2016	**Effective date:**	06-01-2017
Level of Authority:	Laws	**Area of Law:**	Public Security,Post and Telecommunications

Order of the President of the People's Republic of China

中华人民共和国主席令

(No. 53)

（第五十三号）

The Cybersecurity Law of the People's Republic of China, as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016, is hereby issued and shall come into force on June 1, 2017.

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

President of the People's Republic of China: Xi Jinping

中华人民共和国主席 习近平

November 7, 2016

2016年11月7日

Cybersecurity Law of the People's Republic of China

中华人民共和国网络安全法

(Adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016)

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）

Table of Contents

目录

Chapter I General Provisions

第一章　总　　则

Chapter II Cybersecurity Support and Promotion

第二章　网络安全支持与促进

Chapter III Network Operation Security

第三章　网络运行安全

Section 1 General Provisions

第一节　一般规定

Section 2 Operation Security of Critical Information Infrastructure

第二节　关键信息基础设施的运行安全

Chapter IV Network Information Security

第四章　网络信息安全

Chapter V Monitoring, Early Warning and Emergency Response

第五章　监测预警与应急处置

Chapter VI Legal Liability 第六章 法律责任

Chapter VII Supplementary Provisions 第七章 附 则

Chapter I General Provisions

第一章 总 则

Article 1 This Law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization.

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

Article 2 This Law shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China.

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

Article 3 The state shall lay equal stress on cybersecurity and information-based development, follow the guidelines of positive use, scientific development, legal management and security guarantee, promote the construction of network infrastructure and interconnection, encourage the innovation and application of network technologies, support the cultivation of cybersecurity talents, establish and improve the cybersecurity guarantee system, and enhance the capability to protect cybersecurity.

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

Article 4 The state shall develop and continuously improve cybersecurity strategies, specify the basic requirements and major objectives for guaranteeing cybersecurity, and propose cybersecurity policies, work tasks and measures in key fields.

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

Article 5 The state shall take measures to monitor, defend against and deal with cybersecurity risks and threats from both inside and outside the territory of the People's Republic of China, protect critical information infrastructure from attack, intrusion, interference and damage, punish illegal criminal activities on the network in accordance with the law, and maintain cyberspace security and order.

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

Article 6 The state shall advocate honest, faithful, healthy and civilized network conduct, advance the spreading of core socialist values, and take measures to enhance the awareness and level of cybersecurity of the entire society, so as to form a favorable environment for promoting cybersecurity with the participation of the entire society.

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

Article 7 The state shall actively carry out international exchange and cooperation in terms of cyberspace governance, research and development of network technologies, formulation of standards thereof, and crackdown on illegal crimes committed on the network and other aspects, promote the construction of a peaceful, safe, open and

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网

cooperative cyberspace, and establish a multilateral, democratic and transparent system for cyber governance.

络空间，建立多边、民主、透明的网络治理体系。

Article 8 The national cyberspace administration shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration. The competent telecommunications department of the State Council, public security departments and other relevant authorities shall be responsible for cybersecurity protection, supervision and administration within the scope of their respective functions in accordance with the provisions of this Law and other relevant laws and administrative regulations.

第八条　国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

The cybersecurity protection, supervision and administration functions of relevant departments of local people's governments at or above the county level shall be determined in accordance with relevant provisions of the state.

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

Article 9 Network operators shall, when conducting business operations and providing services, abide by laws and administrative regulations, respect social morality, observe business ethics, have good faith, perform the cybersecurity protection obligation, accept supervision by the government and the public, and undertake social responsibilities.

第九条　网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

Article 10 For the construction and operation of the network or the provision of services through the network, technical measures and other necessary measures shall be taken in accordance with the provisions of laws and administrative regulations and the compulsory requirements of national standards to ensure the safe and stable operation of the network, effectively respond to cybersecurity incidents, prevent illegal criminal activities committed on the network, and maintain the integrity, confidentiality and availability of network data.

第十条　建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

Article 11 Network-related industry organizations shall, in accordance with their charters, intensify industry self-discipline, formulate codes of conduct on cybersecurity, direct their members to strengthen cybersecurity protection, raise the level of cybersecurity protection, and promote the sound development of the industry.

第十一条　网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

Article 12 The state shall protect the rights of citizens, legal persons and other organizations to use the network in accordance with the law, promote the popularity of network access, provide better network services, provide the public with safe and convenient network services, and guarantee the orderly and free flow of network information in accordance with the law.

第十二条　国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

Any individual or organization using the network shall comply with the Constitution and laws, follow public order and respect social morality, shall not endanger cybersecurity, and shall not use the network to conduct any activity that endangers national security, honor and interest, incites to subvert the state power or overthrow the socialist

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分

system, incites to split the country or undermine national unity, advocates terrorism or extremism, propagates ethnic hatred or discrimination, spreads violent or pornographic information, fabricates or disseminates false information to disrupt the economic and social order, or infringes upon the reputation, privacy, intellectual property rights or other lawful rights and interests of any other person.

裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

Article 13 The state shall support the research and development of network products and services that are conducive to the healthy growth of minors, legally punish the activities that damage the physical and mental health of minors by using the network, and provide a safe and healthy network environment for minors.

第十三条　国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

Article 14 Any individual or organization shall have the right to report the conduct that endangers cybersecurity to the cyberspace administration, telecommunications department, public security authority, and other departments. The department that receives the report shall handle such a report in a timely manner in accordance with the law, or transfer the report to the competent department in a timely manner if it falls outside its responsibility.

第十四条　任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

The relevant department shall keep confidential the information on the informant, and protect the informant's lawful rights and interests.

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

Chapter II Cybersecurity Support and Promotion

第二章　网络安全支持与促进

Article 15 The state shall establish and improve the system of cybersecurity standards. The standardization administrative department of the State Council and other relevant departments of the State Council shall, according to their respective functions, organize the formulation of and revise at appropriate time national and industry standards relating to cybersecurity administration and the security of network products, services and operations.

第十五条　国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

The state shall support enterprises, research institutions, institutions of higher learning, and network-related industry organizations in participating in the formulation of national and industry standards on cybersecurity.

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

Article 16 The State Council and people's governments of provinces, autonomous regions and municipalities directly under the Central Government shall make overall planning, increase input, support key cybersecurity technology industries and projects, support the research, development and application of cybersecurity technologies, popularize safe and reliable network products and services, protect the intellectual property rights of network technologies, and support enterprises, research institutions, and institutions of higher learning, among others, in participating in national innovation projects on cybersecurity technologies.

第十六条　国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

Article 17 The state shall boost the construction of a socialized service system for cybersecurity, and encourage relevant enterprises and institutions to provide such security services as cybersecurity authentication, detection and risk assessment.

第十七条　国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

Article 18 The state shall encourage the development of technologies for protecting and using network data, promote the availability of public data resources, and promote technological innovation and social and economic development.

第十八条　国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

The state shall support the innovation of cybersecurity management methods and the application of new network technologies to enhance cybersecurity protection.

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

Article 19 People's governments at all levels and their relevant departments shall organize regular cybersecurity publicity and education, and direct and urge relevant entities to conduct cybersecurity publicity and education in an effective manner.

第十九条　各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

Mass media shall offer pertinent cybersecurity publicity and education to the public.

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

Article 20 The state shall provide support to enterprises, institutions of higher learning, vocational schools and other education training institutions to conduct cybersecurity-related education and training, take multiple means to cultivate cybersecurity talents, and promote the exchange of cybersecurity talents.

第二十条　国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

Chapter III Network Operation Security

第三章　网络运行安全

Section 1 General Provisions

第一节　一般规定

Article 21 The state shall implement the rules for graded protection of cybersecurity. Network operators shall, according to the requirements of the rules for graded protection of cybersecurity, fulfill the following security protection obligations, so as to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified.

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

(1) Developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection.

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

(2) Taking technical measures to prevent computer viruses, network attack, network intrusion and other acts endangering cybersecurity.

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

(3) Taking technical measures to monitor and record the status of

（三）采取监测、记录网络运行状态、

network operation and cybersecurity incidents, and preserving relevant weblogs for not less than six months as required.

网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

(4) Taking measures such as data categorization, and back-up and encryption of important data.

（四）采取数据分类、重要数据备份和加密等措施；

(5) Performing other obligations as prescribed by laws and administrative regulations.

（五）法律、行政法规规定的其他义务。

Article 22 Network products and services shall comply with the compulsory requirements of relevant national standards. Providers of network products and services shall not install malware. When a provider discovers any risk such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures, inform users in a timely manner, and report it to the competent department in accordance with relevant provisions.

第二十二条　网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

Providers of network products and services shall continuously provide security maintenance for their products and services, and shall not terminate the provision of security maintenance within the stipulated period or the period agreed upon by the parties.

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

Where network products and services have the function of collecting users' information, their providers shall explicitly notify their users and obtain their consent. If any user's personal information is involved, the provider shall also comply with this Law and the provisions of relevant laws and administrative regulations on the protection of personal information.

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

Article 23 Key network equipment and specialized cybersecurity products shall, in accordance with the compulsory requirements of relevant national standards, pass the security certification conducted by qualified institutions or meet the requirements of security detection before being sold or provided. The national cyberspace administration shall, in conjunction with relevant departments of the State Council, develop and release the catalogue of key network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security detection results to avoid repeated certification and detection.

第二十三条　网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

Article 24 Where network operators provide network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide true identity information when signing agreements with users or confirming the provision of services. If any user fails to provide his or her true identify information, the network operator shall not provide him or her with relevant services.

第二十四条　网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

The state shall implement the strategy of credible identity in

国家实施网络可信身份战略，支持研究

cyberspace, support the research and development of safe and convenient technologies for electronic identity authentication, and promote mutual recognition among different electronic identity authentication technologies.

开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

Article 25 Network operators shall make emergency response plans for cybersecurity incidents, and deal with system bugs, computer viruses, network attack, network intrusion and other security risks in a timely manner. When any incident endangering cybersecurity occurs, the relevant operator shall immediately initiate the emergency response plan, take corresponding remedial measures, and report it to the competent department in accordance with relevant provisions.

第二十五条　网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

Article 26 Such activities as cybersecurity authentication, detection and risk assessment shall be conducted, and cybersecurity information on system bugs, computer viruses, network attack, and network intrusion, among others, shall be released to the public in accordance with relevant provisions of the state.

第二十六条　开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

Article 27 No individual or organization may conduct any activity endangering cybersecurity, such as illegally intruding into any other person's network, interfering with the normal functions of any other person's network, and stealing network data, or provide programs or tools specifically used for conducting activities endangering cybersecurity, such as network intrusion, interference with normal functions and protective measures of the network, and stealing of network data. Whoever knows that any other person conducts any activity endangering cybersecurity shall not provide technical support, advertising promotion, payment and settlement services or any other assistance to such a person.

第二十七条　任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

Article 28 Network operators shall provide technical support and assistance to public security authorities and state security authorities in legally safeguarding state security and investigating crimes.

第二十八条　网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

Article 29 The state shall support cooperation among network operators in such aspects as collection, analysis, and notification of cybersecurity information and emergency response, so as to enhance the capability of network operators to safeguard security.

第二十九条　国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

Relevant industry organizations shall establish and improve cybersecurity protection regulations and cooperation mechanisms for their industries, strengthen the analysis and assessment of cybersecurity risks, give risk warnings to their members on a periodical basis, and support and assist members in responding to cybersecurity risks.

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

Article 30 The information obtained by cyberspace administrations and relevant departments in the performance of cybersecurity protection

第三十条　网信部门和有关部门在履行网络安全保护职责中获取的信息，

functions may not be used for any purpose other than maintaining cybersecurity.

只能用于维护网络安全的需要，不得用于其他用途。

Section 2 Operation Security of Critical Information Infrastructure

第二节　关键信息基础设施的运行安全

Article 31 The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the critical information infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the critical information infrastructure that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council.

第三十一条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

Article 32 The departments in charge of the security protection of critical information infrastructure shall, according to the division of functions prescribed by the State Council, work out and organize the implementation of critical information infrastructure security plans for their industries and fields respectively, and direct and oversee the protection of operation security of critical information infrastructure.

第三十二条　按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

Article 33 In constructing critical information infrastructure, it shall be ensured that such infrastructure has the function of supporting stable and continuous business operation, and that technical security measures are planned, developed and used at the same time.

第三十三条　建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

Article 34 In addition to that prescribed in Article 21 of this Law, critical information infrastructure operators shall also fulfill the following security protection obligations:

第三十四条　除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

(1) Establishing special security management institutions and designating persons in charge of security management, and reviewing the security background of the said persons in charge and personnel on key positions.

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

(2) Conducting cybersecurity education, technical training and skill assessment for employees on a periodical basis.

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

(3) Making disaster recovery backups of important systems and databases.

（三）对重要系统和数据库进行容灾备份；

(4) Making emergency response plans for cybersecurity incidents, and organizing drills on a periodical basis.

（四）制定网络安全事件应急预案，并定期进行演练；

(5) Performing other obligations prescribed by laws and administrative regulations.

（五）法律、行政法规规定的其他义务。

Article 35 Where critical information infrastructure operators purchase network products and services, which may affect state security, they shall pass the state security review organized by the national cyberspace administration in conjunction with relevant departments of the State Council.

第三十五条　关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

Article 36 To purchase network products and services, critical information infrastructure operators shall, in accordance with relevant provisions, enter into security confidentiality agreements with the providers to specify security and confidentiality obligations and responsibilities.

第三十六条　关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

Article 37 Personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of the People's Republic of China shall be stored within China. If it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.

第三十七条　关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

Article 38 Critical information infrastructure operators shall conduct detection and assessment of their cybersecurity and potential risks on their own or entrust cybersecurity service institutions to do so at least once a year; and report the detection and assessment information as well as improvement measures to the relevant department in charge of the security protection of critical information infrastructure.

第三十八条　关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

Article 39 The national cyberspace administration shall make overall planning and coordinate relevant departments to take the following measures to protect the security of critical information infrastructure:

第三十九条　国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

(1) Conducting spot check on the security risks of critical information infrastructure, and proposing improvement measures; if necessary, may entrust cybersecurity service institutions to conduct the detection and assessment of potential security risks of the network.

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

(2) Periodically organizing critical information infrastructure operators to conduct emergency cybersecurity drills, and enhancing the level and capability of coordination and cooperation to respond to cybersecurity incidents.

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

(3) Promoting the sharing of cybersecurity information among relevant departments, critical information infrastructure operators, relevant research institutions, and cybersecurity service institutions, among others.

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

(4) Providing technical support and assistance for emergency response to cybersecurity incidents and the recovery of network functions, among others.

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

Chapter IV Network Information Security

第四章　网络信息安全

Article 40 Network operators shall strictly keep confidential users' personal information collected by them, and establish and improve the system for the protection of users' information.

第四十条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

Article 41 To collect and use personal information, network operators shall follow the principles of legality, rightfulness and necessity, disclose the rules for collection and use, explicitly indicate the purposes, means and scope of collecting and using information, and obtain the consent of the persons whose information is collected.

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

Network operators shall not collect personal information irrelevant to the services provided by them, shall not collect or use personal information in violation of the provisions of any law or administrative regulation or the agreement of both parties, and shall dispose of personal information preserved by them in accordance with the provisions of laws and administrative regulations and agreements with users.

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

Article 42 Network operators shall not divulge, tamper with or damage the personal information collected by them, and shall not provide personal information to any other person without the consent of the persons whose information is collected, except that the information has been processed in a manner that it is impossible to distinguish a specific person and it cannot be retraced.

第四十二条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

Network operators shall take technical measures and other necessary measures to ensure the security of personal information collected by them, and prevent information leakage, damage and loss. In the event that personal information has been or is likely to be divulged, damaged or lost, the operator shall immediately take remedial measures, and inform users in a timely manner and report it to the competent department according to relevant provisions.

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

Article 43 Where an individual finds that any network operator collects or uses his or her personal information in violation of the provisions of any law, administrative regulation or the agreement of both parties, the individual shall be entitled to request the network operator to delete his or her personal information. If the individual finds that his or her personal information collected or stored by the network operator has any error, he or she shall be entitled to request the network operator to make corrections. The network operator shall take measures to delete the information or correct the error.

第四十三条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

Article 44 No individual or organization may acquire personal information by stealing or any other illegal means, or illegally sell or provide personal information to any other person.

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

Article 45 The departments assuming cybersecurity supervision and administration functions in accordance with the law and their staff members shall strictly keep confidential the personal information, privacy and trade secrets to which they have access in performing their functions, and shall not divulge, sell or illegally provide the information to any other person.

第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

Article 46 Any individual or organization shall be responsible for their acts when using the network, shall not set up any website or communications groupfor committing fraud, teaching others how to commit a crime, producing or selling any prohibited or controlled article, or committing any other illegal or criminal activity, and shall not use the network to release the information involving commission of any illegal or criminal activity such as fraud, and the production or sale of any prohibited or controlled article.

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

Article 47 Network operators shall strengthen the management of information released by their users. If any operator finds any information of which the release or transmission is prohibited by any law or administrative regulation, it shall immediately cease the transmission of such information, take deletion or any other handling measure to prevent the information from spreading, preserve relevant records, and report it to the competent department.

第四十七条　网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

Article 48 The electronic information sent by and application software provided by any individual or organization shall not be installed with malware, or contain any information of which the release or transmission is prohibited by any law or administrative regulation.

第四十八条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

Electronic information release service providers and application software download service providers shall perform security management obligations. If a provider finds that any user commits any conduct as set forth in the preceding paragraph, it shall cease the provision of services, take deletion or any other handling measure, preserve relevant records, and report it to the competent department.

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

Article 49 Network operators shall establish complaint and reporting systems for network information security, disclose the ways for filing complaints and reports and other information, and accept and handle complaints and reports related to network information security in a timely manner.

第四十九条　网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

Network operators shall cooperate with the supervision and inspection conducted by cyberspace administrations and relevant departments in accordance with the law.

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

Article 50 The national cyberspace administration and relevant departments shall perform the functions of supervision and administration of network information security in accordance with the law, and shall, when finding any information of which the release or transmission is prohibited by any law or administrative regulation, require the relevant network operator to cease transmission, take deletion or any other handling measure, and preserve relevant records. If the aforesaid information comes from outside the territory of the People's Republic of China, they shall notify the relevant institution to take technological measures and other necessary measures to block the transmission of the information.

第五十条　国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

Chapter V Monitoring, Early Warning and Emergency Response

第五章　监测预警与应急处置

Article 51 The state shall establish systems for cybersecurity monitoring and early warning and information notification. The national cyberspace administration shall make overall planning and coordinate relevant departments to strengthen the collection, analysis and notification of cybersecurity information, and shall uniformly release cybersecurity monitoring and early warning information in accordance with relevant provisions.

第五十一条　国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

Article 52 The departments in charge of critical information infrastructure security protection shall establish and improve the systems for cybersecurity monitoring and early warning and information notification in their respective industries and fields, and report cybersecurity monitoring and early warning information according to relevant provisions.

第五十二条　负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

Article 53 The national cyberspace administration shall coordinate relevant departments to establish and improve the work mechanism for cybersecurity risk assessment and emergency response, make emergency response plans for cybersecurity incidents, and organize drills on a periodical basis.

第五十三条　国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

The departments in charge of critical information infrastructure security protection shall make emergency response plans for cybersecurity incidents in their respective industries and fields, and organize drills on a periodical basis.

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

In emergency response plans for cybersecurity incidents, cybersecurity incidents shall be graded based on such factors as the degree of harm and the scope of influence after the incidents occur, and corresponding emergency response measures shall be prescribed.

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

Article 54 When the probability of cybersecurity incidents increases, relevant departments of people's governments at or above the provincial level shall, according to the prescribed powers and

第五十四条　网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据

procedures as well as the features and possible harm of cybersecurity risks, take the following measures:

网络安全风险的特点和可能造成的危害，采取下列措施：

(1) Requiring relevant departments, institutions and personnel to collect and report relevant information in a timely manner, and strengthen the monitoring of cybersecurity risks.

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

(2) Organizing relevant departments, institutions and professionals to analyze and assess cybersecurity risk information and predict the likelihood of occurrence of, scope of influence of and degree of harm from the incidents.

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

(3) Releasing early warnings on cybersecurity risks to the public and announcing measures to prevent and mitigate the harm therefrom.

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

Article 55 Where any security incident occurs, the emergency response plan for cybersecurity incidents shall be initiated immediately to investigate and assess the incident, and the relevant network operator shall be required to take technical measures and other necessary measures to eliminate potential security hazards and prevent the expansion of the harm, and release to the public the warning information relating to them in a timely manner.

第五十五条　发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

Article 56 Where the relevant department of the people's government at or above the provincial level finds any relatively high security risk or security incident on the network in the performance of cybersecurity supervision and administration functions, it may hold an interview with the legal representative or primary person in charge of the network operator according to prescribed powers and procedures. The network operator shall take measures to make rectification and eliminate hidden risks as required.

第五十六条　省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

Article 57 Emergencies or work safety accidents caused by cybersecurity incidents shall be handled in accordance with the provisions of the Emergency Response Law of the People's Republic of China, the Work Safety Law of the People's Republic of China, and other relevant laws and administrative regulations.

第五十七条　因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

Article 58 For the purposes of maintaining national security and social public order, and handling major social security incidents, with the decision or approval of the State Council, competent departments may take restriction and other temporary measures against network communications in specific regions.

第五十八条　因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

Chapter VI Legal Liability

第六章　法律责任

Article 59 Where any network operator fails to perform the cybersecurity protection obligations as prescribed by Articles 21 and 25 of this Law, the competent department shall order it to take corrective

第五十九条　网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令

action and give it a warning. If the operator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined not less than 10,000 yuan but not more than 100,000 yuan, and its directly responsible person in charge shall be fined not less than 5,000 yuan but not more than 50,000 yuan.

改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

Where any critical information infrastructure operator fails to perform the cybersecurity protection obligations as prescribed by Articles 33, 34, 36 and 38 of this Law, the competent department shall order it to take corrective action and give it a warning. If the operator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined not less than 100,000 yuan but not more than one million yuan, and its directly responsible person in charge shall be fined not less than 10,000 yuan but not more than 100,000 yuan.

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

Article 60 Whoever commits any of the following conduct in violation of the provision of paragraph 1 or 2 of Article 22, or paragraph 1 of Article 48 of this Law shall be ordered to take corrective action and be given a warning by the competent department. If the violator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined not less than 50,000 yuan but not more than 500,000 yuan, and its directly responsible person in charge shall be fined not less than 10,000 yuan but not more than 100,000 yuan.

第六十条　违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

(1) It sets up any malware.

（一）设置恶意程序的；

(2) It fails to immediately take remedial measures or fails to inform users in a timely manner and report it to the competent department in accordance with relevant provisions when it finds any security defect, vulnerability or any other risk of its products or services.

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

(3) It terminates the provision of security maintenance for its products or services without approval.

（三）擅自终止为其产品、服务提供安全维护的。

Article 61 Where a network operator, in violation of the provision of paragraph 1 of Article 24 of this Law, fails to require any user to provide his or her true identity information, or provides related services to any user who fails to provide his or her true identity information, the competent department shall order it to take corrective action; if it fails to take corrective action or the circumstances are serious, it shall be fined not less than 50,000 yuan but not more than 500,000 yuan, and the competent department may order it to suspend relevant business operation, cease business operation for rectification, or close down the website, or may revoke the relevant business permit or business license, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons.

第六十一条　网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Article 62 Where any operator, in violation of the provision of Article 26

第六十二条　违反本法第二十六条

of this Law, conducts cybersecurity authentication, detection, risk assessment or any other activity, or releases to the public any cybersecurity information on system bug, computer virus, network attack or network intrusion, among others, the competent department shall order it to take corrective action and give it a warning; if it fails to take corrective action or the circumstances are serious, it shall be fined not less than 10,000 yuan but not more than 100,000 yuan, and the competent department may order it to suspend relevant business operation, cease business operation for rectification, or close down the website, or may revoke the relevant business permit or business license, and impose a fine of not less than 5,000 yuan but not more than 50,000 yuan on its directly responsible person in charge and other directly liable persons.

规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

Article 63 Where any person, in violation of the provision of Article 27 of this Law, conducts any activity endangering cybersecurity, provides any program or tool specifically used for conducting any activity endangering cybersecurity, or provides technical support, advertising promotion, payment and settlement services or any other assistance to any other person conducting any activity endangering cybersecurity, the public security authority shall, if such act does not constitute a crime, confiscate the violator's illegal income therefrom, detain the violator for not more than five days, and may impose a fine of not less than 50,000 yuan but not more than 500,000 yuan on the violator. If the circumstances are relatively serious, the violator shall be detained for not less than five days but not more than 15 days and may be fined not less than 100,000 yuan but not more than one million yuan.

第六十三条　违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

Where an entity commits any conduct as mentioned in the preceding paragraph, the public security authority shall confiscate its illegal income, impose a fine of not less than 100,000 yuan but not more than one million yuan on it, and punish its directly responsible person in charge and other directly liable persons in accordance with the provisions of the preceding paragraph.

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

The person who is given a public security punishment due to his or her violation of Article 27 of this Law shall not hold the key position of cybersecurity management and network operation within five years; and the person who is given any criminal punishment shall be prohibited for life from holding the key position of cybersecurity management and network operation.

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

Article 64 Where any network operator or provider of network products or services, in violation of any provision of paragraph 3 of Article 22, and Articles 41 throughout 43 of this Law, infringes upon the right that personal information shall be protected in accordance with the law, the competent department shall order it to take corrective action, and may, either separately or concurrently, give it a warning, confiscate its illegal income therefrom, impose a fine of not less than one time but not more

第六十四条　网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚

than ten times the amount of illegal income on it as the case may be, and if it has no illegal income therefrom, impose a fine of not more than one million yuan on it, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons. If the circumstances are serious, the competent department may order it to suspend relevant business operation, cease business operation for rectification, or close down the website, or may revoke the relevant business permit or business license.

款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

Where anyone, in violation of the provision of Article 44 of this Law, acquires personal information by stealing or any other illegal means, or illegally sells or provides personal information to any other person, the public security authority shall, if such act does not constitute a crime, confiscate its illegal income, and impose a fine of not less than one time but not more than ten times the amount of illegal income on it; and if it has no illegal income therefrom, it shall be fined not more than one million yuan.

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

Article 65 Where a critical information infrastructure operator, in violation of the provision of Article 35 of this Law, uses any network product or service that has not undergone security review or has failed to pass security review, the competent department shall order it to cease the use thereof, and impose a fine of not less than one time but not more than ten times the purchase amount on it, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons.

第六十五条　关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Article 66 Where a critical information infrastructure operator stores network data overseas, or provides network data to the overseas in violation of Article 37 of this Law, the competent department shall order it to take corrective action, give it a warning, confiscate its illegal income, and impose a fine of not less than 50,000 yuan but not more than 500,000 yuan on it, and may order it to suspend relevant business operation, cease business operation for rectification, or close down the website, or may revoke the relevant business permit or business license, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons.

第六十六条　关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Article 67 Where any person, in violation of the provision of Article 46 of this Law, sets up any website or communications group for committing any illegal or criminal activity, or uses the network to release any information involving commission of any illegal or criminal activity, the public security authority shall, if such act does not constitute a crime, detain the violator for not more than five days, and may impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on the violator, and if the circumstances are relatively serious, may detain the violator for not less than five days but not more than 15 days, and may

第六十七条　违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下

impose a fine of not less than 50,000 yuan but not more than 500,000 yuan on the violator. The website or communications group used for committing any illegal or criminal activity shall be shut down.

罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

Where an entity commits any conduct as mentioned in the preceding paragraph, the public security authority shall impose a fine of not less than 100,000 yuan but not more than 500,000 yuan on it, and punish its directly responsible person in charge and other directly liable persons in accordance with the provisions of the preceding paragraph.

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

Article 68 Where a network operator, in violation of the provision of Article 47 of this Law, fails to cease the transmission of the information of which the release or transmission is prohibited by any law or administrative regulation, take deletion or any other handling measure, and preserve relevant records, the competent department shall order it to take corrective action, give it a warning, and confiscate its illegal income. If the operator refuses to take corrective action or the circumstances are serious, the competent department shall impose a fine of not less than 100,000 yuan but not more than 500,000 yuan on it, and may order it to suspend relevant business operation, cease business operation for rectification, or close down the website, or may revoke the relevant business permit or business license, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on its directly responsible person in charge and other directly liable persons.

第六十八条　网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Any electronic information release service provider or application software download service provider that fails to perform the security management obligation prescribed in paragraph 2 of Article 48 of this Law shall be punished in accordance with the provisions of the preceding paragraph.

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

Article 69 Where a network operator commits any of the following conduct in violation of the provisions of this Law, the competent department shall order it to take corrective action; and if the operator refuses to take corrective action or the circumstances are serious, it shall be fined not less than 50,000 yuan but not more than 500,000 yuan, and its directly responsible person in charge and other directly liable persons shall be fined not less than 10,000 yuan but not more than 100,000 yuan.

第六十九条　网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

(1) It fails to take such handling measures as ceasing the transmission of and deleting the information of which the release or transmission is prohibited by any law or administrative regulation according to the requirements of the relevant department.

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

(2) It refuses to accept or obstructs the supervision and inspection conducted by the relevant department in accordance with the law.

（二）拒绝、阻碍有关部门依法实施的监督检查的；

(3) It refuses to provide technical support and assistance to any public security authority or state security authority.

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

Article 70 Whoever releases or transmits the information of which the release or transmission is prohibited by paragraph 2 of Article 12 of this Law, or by any other law or administrative regulation shall be punished in accordance with the provisions of relevant laws and administrative regulations.

第七十条　发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

Article 71 Any acts in violation of this Law shall be recorded in credit archives in accordance with the provisions of relevant laws and administrative regulations and be published.

第七十一条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

Article 72 Where the operator of any government affairs network of a state authority fails to perform the cybersecurity protection obligation prescribed in this Law, its superior authority or the relevant authority shall order it to take corrective action, and take disciplinary actions against its directly responsible person in charge and other directly liable persons in accordance with the law.

第七十二条　国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

Article 73 Where the cyberspace administration or the relevant department uses the information obtained in the performance of cybersecurity protection functions for any other purpose in violation of the provision of Article 30 of this Law, its directly responsible person in charge and other directly liable persons shall be subject to disciplinary actions in accordance with the law.

第七十三条　网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

Any staff member of the cyberspace administration or the relevant department who neglects duty, abuses power, practices favoritism, or makes falsification shall, if the act does not constitute a crime, be subject to disciplinary action in accordance with the law.

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

Article 74 Whoever violates the provisions of this Law and causes any damage to any other person shall assume civil liability in accordance with the law.

第七十四条　违反本法规定，给他人造成损害的，依法承担民事责任。

Whoever violates the provisions of this Law shall, if the act constitutes a violation of public security administration, be subject to public security administration punishment in accordance with the law, and if the act constitutes a crime, be subject to criminal liability in accordance with the law.

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

Article 75 Where any overseas institution, organization or individual attacks, intrudes into, disturbs, destroys or otherwise damages the critical information infrastructure of the People's Republic of China, causing any serious consequence, the violator shall be subject to legal liability in accordance with the law; and the public security department of the State Council and relevant departments may decide to freeze the property of or take any other necessary sanction measure against the institution, organization or individual.

第七十五条　境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

Chapter VII Supplementary Provisions

第七章　附　　则

Article 76 In this Law, the following terms shall have the meanings as follows:

(1) “Network” means the system that consists of computers or other information terminals and related equipment for collecting, storing, transmitting, exchanging, and processing information according to certain rules and procedures.

(2) “Cybersecurity” means the capabilities of, by adoption of necessary measures, preventing network attack, intrusion, interference, and destruction, illegal use of network as well as network incidents, making the network stay in a state of stable and reliable operation, and guaranteeing the integrity, confidentiality and availability of network data.

(3) “Network operator” means the owners and administrators of the network as well as network service providers.

(4) “Network data” means all kinds of electronic data collected, stored, transmitted, processed and generated through the network.

(5) “Personal information” means all kinds of information recorded in an electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person's name, date of birth, identity certificate number, biology-identified personal information, address and telephone number.

Article 77 The protection of operation security of the network storing and processing information involving state secrets shall, in addition to the provisions of this Law, comply with the provisions of laws and administrative regulations on confidentiality.

Article 78 The security protection of military network shall be prescribed by the Central Military Commission separately.

Article 79 This Law shall come into force on June 1, 2017.

第七十六条　本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条　存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条　军事网络的安全保护，由中央军事委员会另行规定。

第七十九条　本法自2017年6月1日起施行。